SCAMP Farrow

LECTURE I - SECTION I

1. Appreciate the opportunity to be a participant of SCAMP '58 and to talk a bit about some of the interesting episodes and important landmarks that stand out in the historical background of the science and/or art of cryptology.

2. In inviting me to speak on the subject I assume that the objective is to deal with that area of the background of cryptology which has primarily to do with its development and manner of employment as a vital military weapon

3 Now cryptology has certainly not always been considered a vital military weapon, or even as a weapon For instance, even as recently as in 1955, when the U.S was trying to help our most important ally in the cultivation of the cryptologic gardens by providing her with the money for the purpose I mentioned just a few months ago, we sought to use funds allocated to MDAP-the Mutual Defense Assistance Pact. But those funds are specifically earmarked for research and development of physical instruments, machines, guns, electronic devices, etc , and it seemed hopeless even to try to justify the use of MDAP montey for crypt-analytic research and development. It was only after we had pointed out the ways in which military cryptology had been used in World War I and II that the funds sought were granted.

4. This point about cryptology being useful only for such relatively unimportant things as personal diaries, love missives, and attempts to prove that Bacon or somebody else wrote the Shakespeare Plays reminds me of a story which may be a bit apochraphyl but is somewhat amusing

5 The story of the old Persian Queen Semiramis

It is planned that I give a series of talks on the highlights of cryptologic history. This may be useful at least to some of the members of SCAMP '58, for I may tell you right away that there doesn't exist in English or in any other language, for that matter, an adequate or even a fairly good history of the invention and development of cryptography and of its counterpart, cryptanalysis.

There is no real history, definitive and detailed. What bits and pieces one finds here and there in popular accounts are generally full of misunderstandings, misstatements, and downright lies.

Of course, there is a good reason why no history of cryptology worthy of the name has been produced for public use It is that as a rule governments don't publish them or permit its cryptologic workers to publish histories, brochures, or articles. This is an understandable and sensible rule if not carried to absurd and illogical limits by insisting that all COMINT must be kept secret for all time. Later on I may tell you about an amusing if not enlightening conference I was summoned to attend at the Pentagon a week ago today.

Of course, now and then some cryptologic information does leak out, as for example, when congressional and other official investigations either require or accidently bring about the disclosure of such information, or when some formerly trusted worker comits indiscretions, or consciously and deliberately breaks the trust that had been imposed. Of both these types of security breaches--official or personal--I shall have more to say later on. At the moment I will merely comment that the history which comes from such leakages and breaches of trust are apt to contain errors, misunderstandings, distortions, and lies.

Some of you may have wondered what the title of my talk or series of talks is. Dean Swift asked me yesterday to tell him so that it could be indicated on the announcement sheet. I told him I preferred to state the title myself and I'll now disclose my secret by telling you that the title is:

"The Influence of C-power on History."

Lest there be some here who think I'm laboring under the delusion that this building and SCAMP are U.S. Navy property or that I've suddenly gone psychotic and imagine I'm Admiral Mahan, I hasten to explain ~~that~~ bogus the "C" in ~~the~~ such a title of my talk is not the word "SEA" but the letter "C" and it stands for the word CRYPTOLOGIC. The title of the talk ~~is~~ would be therefore "The influence of cryptologic power on history." As a sub-title I would offer this: "Or how to win battles and ~~wars~~ campaigns and go down in history as a great tactician, strategist and leader of men; or, on the other hand, how to lose battles and wars and go down in history as an incompetent commander, ~~a heel,~~ a military 'no-good-nik' "

At this point let me hasten to deny that I'm casting any reflections upon certain successful--spectacularly successful commanders, such as Generals Eisenhower and MacArthur. ~~But~~ names will occur to you without my calling them to your attention--and there will be names of men in each of the two categories--"how to

win" and "how to lose" battles and campaigns — and entire wars, for that matter.

At this point I'm reminded of a story about General Montgomery--"Monty" and I have the story on pretty good authority.

Story re Monty in N. Africa, 1942.

Before a group such as this I think it hardly necessary to make this general statement but Ill make it: That not all historians know that the history of diplomacy and warfare teems with instances where the turn of events was greatly affected by the relative cryptologic power of the opposing forces Most of the history in the history books, especially when first written, does not tell the complete story or the whole truth -- for the cryptologic facts are usually ver carefully hidden from historians, even from official historians, and are not brought to light for years, decades, centuries, and maybe never (Tell about (1) Morison (Samuel Eliot), (2) Navy Op. Research on Battle of Atlantic; (3) Wenger lecture at Naval War College

Sometimes the course of history is materially or drastically changed by the amount and quality of the communications intelligence, COMINT for short, and communications security, COMSEC for short, commanders have had available to them and how they used these offensive and defensive weapons. Consider, for example, the existence of COMINT, or it could have been changed by its proper use--as some say it did, the COMINT available to us before Pearl Harbor, but sometimes, also, the amount and quality of the and what use was made of it. Consider also, for example, the effect of the absence of COMINT in the Battle of the Bulge, to which I'll return later in my talk. At the moment let course of history is materially changed by the non-existence of COMINT where it had previously existed and was used. We will discuss an incident of the latter type

as I consider too, in due course. But first, an incident of the former type--Pearl Harbor. The story of Pearl Harbor, which I begin by reading from the 17 December 1945 issue of TIME, I should preface the reading by reminding you that the war was over--or at least V-E and V-J days had been celebrated--and the clamor on the part of vociferous Republicans, who had for years been insisting upon learning and disclosing to the world the reasons why we had been caught by surprise in such a disastrous defeat and calamity as the Japanese had inflicted upon us at Pearl. This clamor had to be met. It could no longer be hushed by the need for military secrecy. So there were investigations--a half dozen or more, winding up in a grand finale of the Joint Congressional Investigation into the Attack on Pearl Harbor. It was this investigation which not only itself brought into the open every detail and exhibit in its own lengthy investigation and hearings but also disclosed everything that was said and shown at all the previous Army and Navy investigations--about a half dozen of them.

There came a day in the Congressional Hearings when General George C. Marshall, Chief of Staff, U.S. Army at the time of the Pearl Harbor Attack, was called to the witness stand. He testified for several days, long, long ones. Toward the end of the ordeal he was questioned about a letter it had been rumored he'd written

to Governor Dewey in the Autumn of 1944, during the Presidential Campaign. General Marshall balked. He pleaded most earnestly with the Committee not to force him to disclose the letter or its contents, but to no avail. He had to bow to the will of the Committee.

Read TIME to "Uneasy Secret".

A few moments ago I commented that the sort of cryptologic history which gets published as a result of official investigations is apt to contain errors, misunderstandings, distortions, and downright lies. And this account in TIME contains its share of them. But the curious part of this story is that TIME didn't commit these offenses, they were in the original Marshall-Dewey letter, which had been prepared by somebody on Marshall's staff who got the results of COMINT but was no technician or cryptologist I will interrupt the reading of the letter to remark that undoubtedly those of you who followed at all closely the disclosures--the remarkable and shocking disclosures from the point of view of national security--of the Joint Congressional Investigation of the Attack on Pearl Harbor must have wondered about or been mystified by this question: If we were really reading the Japanese code long before Pearl Harbor, why were we caught by surprise when the attack came? Why did we lose over 3,000 men in a couple of hours, all those big

battleships in harbor, and all those planes on the ground?

You weren't alone in thinking about this mystery Listen to these extracts from the Report of the Majority of that Joint Congressional Committee, p. 17Ø & 253

I'll return later to the Marshall-Dewey correspondence. But now:

What was meant by the name "MAGIC"?

How did the term come to be used?

~~It was introduced into our usage by the British~~ first used by the British and then introduced into our usage

It was the cover name during WW II years for the product of COMINT operations and activities. (1) Special intelligence, (2) Traffic intelligence, (3) Weather intelligence

I suppose its hardly necessary for me to tell you how carefully guarded were the fruits of the MAGIC--even the fact of its existence was known to only a very few persons. Hearings p. 261 Success--rather its continuance--rested upon a very slender thread

Midway, for instance, Marshall-Dewey letter

(J Red machine. OSS in Lisbon. Marshall-Dewey ltr.)

There are many persons who still argue about certain questions about Pearl Harbor. Every so often the story comes up and the fires of controversy are fanned

once again to the blazing point (A researcher at RAND is still working on a rather lengthy treatise on the subject.) The right-wingers are, of course, still convinced and are trying to convince other Americans that President Roosevelt brought the attack about and deliberately Some of them make shocking charges and allegations of conspiracy among Roosevelt, Marshall and Stark. Which of course is nonsense--disprovable by rather easy logic. Maybe I'll go into this later if you wish

But let's get back to the Marshall-Dewey letter

The harm that the disclosure of this letter caused is incalculable. The hearings were open and the documents (40 volumes) are public documents.

Should we be greatly astonished that certain governments have greatly improved their communications security devices and arrangements since the close of the Congressional Investigations??????

I read now from p. 232 of the Majority Report of the Joint Congressional Committee.

1 " . all witnesses familiar with MAGIC material throughout the war have testified that it contributed enormously to the defeat of the enemy, greatly shortened the war, and saved many thousands of lives "

2. General Chamberlin (G-3 of Gen. MacArthur's staff throughout the war in the Pacific (told me (and he put it in writing for me on request): "The information G-2 gave G-3 in the Pacific theater alone saved us many thousands of lives and shortened the war by no less than two years "

3 I hardly need say what the latter saving alone was worth in billions of dollars. I made a calculation and found that $1.ØØ spent for COMINT equals $1,ØØØ spent for other war materials and activities.

Now let's see what happened during WW II when we had and didn't have COMINT on our side.

In our struggle against two very desperate enemies, the Germans and the Japanese, it was often the possession of COMINT, the so-called "MAGIC" which meant the difference between defeat and success. When we had magic we could put what little we had at the right time in the right place And when we didn't have it--as in the famous and almost terribly disastrous Battle of the Bulge we took a bad beating.

Josh Cooper's remarks on the
- READ from ~~letter~~ ^ of "Effigy"
on G-2 & G-3 Forces

When we didn't have it--well, as I said, things went badly because our principal G-2's had come to rely too heavily on it.

The Battle of the Bulge
Baldwin Article - Read.

1. Show 1st page of Baldwin article. (p. 3Ø) and read title of.

2. Read from next card -- Merriam.

3. Then read extracts from p 4Ø.

Extract from: Merriam, Robert E., Dark December: The full account of the Battle of the Bulge, 1947-Ziff-Davis Publishing Co., p. 211:

"According to Eisenhower's personnel officer, American losses in the Battle of the Bulge totalled 75,89Ø men, of whom 8,6Ø7 were killed, 47,139 wounded, and 21,144 missing Over 8,ØØØ of these casualties were in the 1Ø6th Division. Because of heavy German attacks, 733 tanks and tank destroyers were lost. Two divisions, the 28th and 1Ø6th, were nearly completely annihilated, although the 28th Division did subsequently enter combat after being rebuilt."

I hope I've not tired you out by such a lengthy preface to the real substance of my talks. So we'll begin by asking:

How old is the science of cryptology?

Which camefirst -- secret writing?

Or plain-text writing?

The art of writing probably grew out of pictographs and its growth can be traced back to the dawn of civilized man. Rebuses.

4 12
Example of rebus (p.2)

Cryptanalysis - and psychoanalysis - in the Bible.

Nebuchadnezzar and his dream. Daniel, Chapter 2: 3,4,5,6,7,8,9,1Ø,11.

Belshazzar - Daniel, Chapter 5: 1-5, 25-30

Read from Bible - Daniel

MENE, MENE, TEKEL (UPHARS IN / PERES

Belshazzar and "The Handwriting on the Wall".

Daniel - The first cryptanalyst (B.C. 570-569)

The Second Psychoanalyst or interpreter of dreams. Joseph was first.

Instances of actual cipher in the Bible:

1

Jeremiah 25:26
51:41

2

Scytale

Some history from British Manual of Cryptography.

Scytale - Spartan Ephors send messages to commanders in field. Example from Grecian history. Greek at Court of Persian King Darius--message to colleague Aristagoras in Greece.

Conveying info in wartime by bundles of ribands of different colors, notches on stick, knots tied in various ways Fires or beacons--all nations of antiquity.

Polybius describes system used by Greeks--co-ordinate system--Letters divided into groups of five and the number of fires lit in two separate places denoted the

group of letters and the position of the letter in that group. Fires as late as 1746 in Italy to signal; code given to General the Marquis de Mirepoix in command mixed corps French, Spanish and Genoese troops, still in existence.

In Africa--beating of drums--only chiefs of tribes and headman initiated.

Ceasar's cipher - invented and used many centuries earlier in various countries -- by Carthagenians and Phoenicians. Used by Germans in 1870-71 and by British forces during S African war

The only systems known to have been employed between time of Julius Caesar and the beginning of the 16th Century are two:

1 i = . a = : e = :. o = :: u = :.:

Th: t::wn c:p.t. .l:t: d

2. System in which consonants remain unaltered but the vowels are replaced by the immediately following consonant.

For many centuries after Roman invasion British crypt almost entirely neglected, one reason being that the art of secret writing was long regarded as an invention of the Evil One. There are many instances of students of it being accused of sorcery, among whom may be mentioned Trithemius the Abbe of Spanheim . . .

p. 6 - British Manual of Cryptography. Read

Viete - Then about him. P. 6 British Manual.

1

Correspondence between Court of Spain Henri IV (1553-1610) and Chiefs Anti-Royalists in France.

3.1
RUNES on a stone in front of Gripsholm Castle near Stockholm.

A.S "Rune" - "a secret, a myster." "Magic".

Any of the characters of the alphabet formerly in general use by the Teutonic, of Germanic, peoples from about the 3d Century A.D.

Blocked out portion -- another type of "Ruin"

Beginnings of modern cryptology can be traced back to the days of the early years of the 15th Century, when it was extensively employed by the princes and chancelleries of the Papal States.

For example, see this alphabet of 1401:

4.10
Cipher alphabet of 1401)

245.2
Trithemuis - 1518.

Abbe of Spanheim

151
Trithemian Oath

Present oath Back up by P.L. 513 - now USC 798.

We administer a special oath to everybody who comes into the field.

1st slide - 242.

246 or 3
Examples of cipher alphabets and small syllabaries used centuries ago.

1. Charlemagne's cipher (768-814)
2. Cipher used in England during reign of Alfred the Great (871-901).

246 3. Ogam writing of ancient Eire
4. Ogam-like alphabet of Charles I (1646) to Marquis of Worcester.

3 5. Marquis of Worcester's "Clock Cipher"
6. Cardinal Wolsey, 1524, Vienna
7. Sir Thomas Smith, Paris, 1563.
8. Sir Thomas Chaloner, Madrid, 1561.
9. Sir Edward Stafford, Madrid, 1586.

3.3
Cipher alphabet in Sir Thomas More's Utopia, 1518.

3.5
Facsimile of a cipher found among the papers of Mary Stuart, Queen of Scots (1542-1587).

3.6
Cipher alphabet - Queen Mary Stuart and Bishop of Glasgow, then her Ambassador or solicitor in France, 1571

3.7
Sliding-card cipher. Facsimile of one used in the later years of Elizabeth's reign (about 1600).

3.8
The two-word square cipher. State cipher used in Charles I's time (1627) for communicating with France and Flanders (A co-ordinate system)

3.9
Part of Duke of Buckingham's cipher used in 1627 for communicating with France.

3.10
Numerical cipher used in reign of Charles II (1630-1685) between Prince Rupert and the Earl of Arlington, Sec. State.

3.11
Foreign Office Cipher during reign of George III (1779)

217
Frontispiece of "The Babington Plot" by Alan Gordon Smith, London 1936. The cipher used by Mary Stuart Queen of Scots with Babington. (1542-1587)

218
Frontispiece of "The Babington Plot" by Smith. The Forged Postscript, with Phillips' endorsement (Ciphers involved in the Babington Plot. The forged postscript)

5.2
Cipher used by Philip II of Spain (1527-1598) reigned 1556-98 (pp. 102, 103).

But monoalphabetic ciphers still used today!

3.4
Gustav Rumrich spy case

6
Porta's table (1563)

6.1
Porta's table as it appears in an early Elizabethan State paper.

5
Vigenere Square as pictured in the ordinary literature.

5.1
Vigenere Square as V. describes it in his book (1586).

104
Ciphers used by Galileo (1564-1642) Italian astronomer and physicist.
Huyghens (1629-1695 Dutch mathematicians, physicist and astronomer

P 9 - British Manual.

One of the earliest instances of the advantage gained in the course of military operations by the capture and subsequent solution of a message sent by the enemy took place in 1626, Siege of Realmont, a town of Languedoc, then in possession of the Huguenots but besieged by the King's troops under command of the Prince de Conde.

Latter about to raise siege. Message intercepted. Rossignol reads. Out of powder and would have to surrender if not immediately received new supply